In the claims:

1. (Previously Presented) A system for securely transforming an audio stream to encoded text, comprising:

a security core which provides security functions;

a plurality of components, comprising at least an audio recording component and one or more transformation components;

a security core operating module configured to operate the security core;

wherein the components are securely operably connected to the security core, such that the security core can vouch for authenticity of each securely operably connected component;

wherein the securely operably connected audio recording component is configured to record an audio stream;

wherein the at least one of the securely operably connected transformation components is configured to transform the audio stream to a text stream;

wherein the security core is configured to securely provide, for the text stream, an identification of the securely operably connected audio recording component and each of the at least one securely operably connected transformation components;

wherein the security core is configured to detect whether the audio recording component and the at least one transformation component remain operably connected to the security core during the recording and the transforming of the audio stream; and

wherein the security core is configured to abort the recording and the transforming if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core during the recording and the transforming of the audio stream.

2. (Original) The system according to claim 1, wherein selected ones of the operable connections are made using one or more buses of the security core.

3. (Original) The system according to claim 1, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security core.

4. (Original) The system according to claim 3, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

5. (Original) The system according to claim 1, wherein selected ones of the secure operable connections are provided when the security core is manufactured.

6. (Currently Amended) The system according to claim 1, wherein the ~~the~~ security core is configured to authenicate the operably connected component.

7. (Currently Amended) The system according to claim 6, wherein the ~~the~~ operably connected component is configured to provide a unique identifier of the operably connected component to the security core, along with a digital signature of the unique identifier that is created using a private key of the operably connected component; and the security core is configured to use a public key that is cryptographically associated with the private key to determine authenticity of the operably connected component.

8. (Currently Amended) The system according to claim 1, wherein the ~~the~~ component is securely operably connected after a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component.

9. (Previously Presented) The system according to claim 7, wherein the unique identifier is securely stored on the operably connected component.

10. (Previously Presented) The system according to claim 6, wherein the security core is authenticated to the operably connected component.

11. (Canceled)

12. (Previously Presented) The system according to claim 1, wherein the security core is configured to mark the text stream as not authenticated if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core during the recording and the transforming of the audio stream.

13. (Previously Presented) The system according to claim 7, wherein the security core is configured to determine whether the audio recording component and the at least one transformation component have been authenticated; and to abort the recording or the transforming if one or more of the audio recording component and the at least one transformation component has not been authenticated to the security core.

14. (Previously Presented) The system according to claim 7, wherein the security core is configured to determine whether the audio recording component and the at least one transformation component have been authenticated to the security core and to mark the text stream as not authenticated if one or more of the audio recording component and the at least one transformation component has not been authenticated to the security core.

15. (Currently Amended) The system according to claim 1, wherein the security core is configured to digitally notarize the text stream.

16. (Previously Presented) The system according to claim 1, wherein the security core is configured to provide an additional data stream that is associated with the text stream, wherein the additional data stream comprises a digital notarization of the text stream.

17. (Previously Presented) The system according to claim 15, wherein the security core is configured to compute a hash value over the text stream to combine the hash value with a unique identifier of the audio recording component and of each of the at least one transformation components, thereby creating a combination data block to hash the combination data block; to sign the hashed combination data block with a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith; and to provide the digitally signed hashed combination data block, along with the combination data block, as the digital notarization for the text stream, wherein the digital notarization cryptographically seals contents of the text stream and identifies the audio recording component and each of the at least one transformation components.

18. (Previously Presented) The system according to claim 17, wherein the security core is configured to verify authenticity of the text stream by a receiver of the text stream and the digital notarization, using the public cryptographic key of the security core, and for concluding that the text stream is authentic if the verification succeeds.

19. (Previously Presented) The system according to claim 18, wherein the security core is configured to conclude that the text stream has not been tampered with if the verification succeeds.

20. (Previously Presented) The system according to claim 18, wherein the security core is configured to verify authenticity by determining the audio recording component and the at least one transformation component involved in creating the text stream by decoding the digitally signed hashed combination data block to reveal the unique identifiers thereof.

21. (Currently Amended) The system according to claim 15, wherein the at least one transformation component comprises an anolog to digital transformation component configured to transform the audio stream to a digital stream, and a speech recognition transformation component configured to convert the digital stream to the text stream and the

security core is configured to compute a hash over the text stream, to combine the hash with unique identifiers of the audio recording component, the analog-to-digital transformation component, and the speech recognition transformation component and to digitally sign the ~~the has~~ hash with unique identifiers using a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith.

22. (Previously Presented) The system according to claim 15, wherein the at least one transformation component comprises an analog-to-digital transformation component, a speech recognition transformation component, an authenticated speaker specific speech recognition database, a lexical transformation component and a text compression transformation component, wherein the analog-to-digital transformation component is configured to transform the audio stream to a first digital stream, the speech recognition transformation component is configured to convert the first digital stream to a first encoded text stream, wherein the speech recognition transformation component is augmented by the lexical transformation component and the authenticated speaker specific speech recognition database; and the text compression transformation component is configured to compress the first encoded text stream into the text stream; and the security core is configured to digitally notarize the text stream by computing a hash over the text stream, and to combine the hash with unique identifiers of: (1) the audio recording component; (2) the analog-to-digital transformation component; (3) the speech recognition transformation component; (4) the authenticated speaker-specific speech recognition database and/or the lexical transformation component (5) the text compression transformation component; and the security core is configured to sign the hash and unique identifies using a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith.

23. (Original) The system according to claim 1, wherein the text stream is an ASCII text stream.

24. (Original) The system according to claim 1, wherein the text stream is an EBCDIC text stream.

25. (Previously Presented) A method of securely transforming an audio stream to encoded text, comprising:

operating a security core which provides security functions;

providing a plurality of components, comprising at least an audio recording component and one or more transformation components;

securely operably connecting the components to the security core, such that the security core can vouch for authenticity of each securely operably connected component;

recording an audio stream by the securely operably connected audio recording component;

transforming the audio stream to a text stream by at least one of the securely operably connected transformation components;

securely providing, for the text stream by the security core, an identification of the securely operably connected audio recording component and each of the at least one securely operably connected transformation components;

detecting whether the audio recording component and the at least one transformation component remain operably connected to the security core during operation of the recording and the transforming of the audio stream; and

aborting the recording and the transforming if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core during the recording and the transforming of the audio stream.

26. (Original) The method according to claim 25, wherein selected ones of the operable connections are made using one or more buses of the security core.

27. (Original) The method according to claim 25, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security core.

28. (Original) The method according to claim 27, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

29. (Original) The method according to claim 25, wherein selected ones of the secure operable connections are provided when the security core is manufactured.

30. (Previously Presented) The method according to claim 25, wherein the securely operably connecting the components to the security core further comprises authenticating the operably connected component to the security core.

31. (Currently Amended) The method according to claim 30, wherein performing the authenticating of the operably connected component to the security core further comprises providing a unique identifier of the operably connected component to the security core, along with a digital signature of the unique identifier that is created using a private key of the operably connected component; and using, by the security core, a public key that is cryptographically associated with the private key to determine authenticity of the operably connected component.

32. (Previously Presented) The method according to claim 25, wherein the securely operably connecting the components to the security core is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component.

33. (Previously Presented) The method according to claim 30, wherein instructions for performing the authenticating of the operably connected component to the security core are securely stored on the operably connected component.

34. (Previously Presented) The method according to claim 30, further comprising authenticating the security core to the operably connected component.

35. (Canceled)

36. (Previously Presented) The method according to claim 25, further comprising detecting whether the audio recording component and the at least one transformation component remain operably connected to the security core during operation of the recording and the transforming of the audio stream; and marking the text stream as not authenticated if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core during operation of the recording and the transforming of the audio stream.

37. (Previously Presented) The method according to claim 31, further comprising determining whether the audio recording component and the at least one transformation component have been authenticated to the security core; and aborting the recording or the transforming if one or more of the audio recording component and the at least one transformation component has not been authenticated to the security core.

38. (Previously Presented) The method according to claim 31, further comprising determining whether the audio recording component and the at least one transformation component have been authenticated to the security core; and marking the text stream as not authenticated if one or more of the audio recording component and the at least one transformation component has not been authenticated to the security core.

39. (Previously Presented) The method according to claim 25, wherein the securely providing, for the text stream by the security core, an identification of the securely operably connected audio recording component and each of the at least one securely operably

connected transformation components further comprises digitally notarizing, by the security core, the text stream.

40. (Previously Presented) The method according to claim 25, wherein the securely providing, for the text stream by the security core, an identification of the securely operably connected audio recording component and each of the at least one securely operably connected transformation components further comprises providing an additional data stream that is associated with the text stream, wherein the additional data stream comprises a digital notarization, created by the security core, of the text stream.

41. (Previously Presented) The method according to claim 39, wherein the digitally notarizing further comprises computing, by the security core, a hash value over the text stream; combining the hash value with a unique identifier of the audio recording component and of each of the at least one transformation components, thereby creating a combination data block; hashing the combination data block; digitally signing the hashed combination data block with a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith; and providing the digitally signed hashed combination data block, along with the combination data block, as the digital notarization for the text stream, wherein the digital notarization cryptographically seals contents of the text stream and identifies the audio recording component and each of the at least one transformation components.

42. (Previously Presented) The method according to claim 41, further comprising verifying authenticity of the text stream by a receiver of the text stream and the digital notarization, using the public cryptographic key of the security core, and concluding that the text stream is authentic if the verification succeeds.

43. (Previously Presented) The method according to claim 42, wherein the verifying authenticity of the text stream further comprises concluding that the text stream has not been tampered with if the verification succeeds.

44. (Previously Presented) The method according to claim 42, wherein the verifying authenticity of the text stream further comprises the determining the audio recording component and the at least one transformation component involved in creating the text stream by decoding the digitally signed hashed combination data block to reveal the unique identifiers thereof.

45. ((Previously Presented) The method according to claim 39, wherein the transforming the audio stream to a text stream further comprises transforming the audio stream to a digital stream by a first of the at least one transformation components which is an analog-to-digital transformation component; and converting the digital stream to the text stream by a second of the at least one transformation components which is a speech recognition transformation component; and the digitally notarizing the text stream further comprises computing a hash over the text stream; combining the hash with unique identifiers of the audio recording component, the analog-to-digital transformation component, and the speech recognition transformation component; and digitally signing the combination using a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith.

46. (Previously Presented) The method according to claim 39, wherein the transforming the audio stream to a text stream further comprises transforming the audio stream to a first digital stream by a first of the at least one transformation components which is an analog-to-digital transformation component; converting the first digital stream to a first encoded text stream by a second of the at least one transformation components which is a speech recognition transformation component, wherein the speech recognition transformation component may be augmented by zero or more others of the at least one transformation components which are an authenticated speaker-specific speech recognition database and/or a lexical transformation component; and compressing the first encoded text stream into the text stream using a third of the at least one transformation components which is a text compression transformation component; and the digitally notarizing the text stream

further comprises computing a hash over the text stream; combining the hash with unique identifiers of: (1) the audio recording component; (2) the analog-to-digital transformation component; (3) the speech recognition transformation component; (4) the authenticated speaker-specific speech recognition database and/or the lexical transformation component, if they augmented the speech recognition transformation component; (5) the text compression transformation component; and signing the combination using a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith.

47. (Original) The method according to claim 25, wherein the text stream is an ASCH text stream.

48. (Original) The method according to claim 25, wherein the text stream is a Unicode text stream.

49. (Previously Presented) A computer program product for securely transforming an audio stream to encoded text, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code configured to operate a security core which provides security functions;

computer-readable program code configured to securely operably connect one or more components, comprising at least an audio recording component and one or more transformation components, to the security core, such that the security core can vouch for authenticity of each securely operably connected component;

computer-readable program code configured to transform an audio stream that is recorded by the securely operably connected audio recording component to a text stream, the transforming being performed by at least one of the securely operably connected transformation components;

and computer-readable program code configured to securely provide, for the text stream by the security core, an identification of the securely operably connected audio

recording component and each of the at least one securely operably connected transformation components;

computer-readable program code configured to detect whether the audio recording component and the at least one transformation component remain operably connected to the security core during the recording and the transforming; and

computer-readable program code configured to abort the recording and the transforming if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core during the recording and transforming.

50. (Original) The computer program product according to claim 49, wherein selected ones of the operable connections are made using one or more buses of the security core.

51. (Original) The computer program product according to claim 49, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security core.

52. (Original) The computer program product according to claim 51, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

53. (Original) The computer program product according to claim 49, wherein selected ones of the secure operable connections are provided when the security core is manufactured.

54. (Previously Presented) The computer program product according to claim 49, wherein the computer-readable program code configured to securely operably connect further comprises computer-readable program code configured to authenticate the operably connected component to the security core.

55. (Previously Presented) The computer program product according to claim 54, wherein the computer-readable program code configured to authenticate further comprises: computer-readable program code configured to provide a unique identifier of the operably connected component to the security core, along with a digital signature of the unique identifier that is created using a private key of the operably connected component; and computer-readable program code configured to use by the security core, a public key that is cryptographically associated with the private key to determine authenticity of the operably connected component.

56. (Previously Presented) The computer program product according to claim 49, wherein the computer-readable program code configured to securely operably connect is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component.

57. (Previously Presented) The computer program product according to claim 54, wherein the computer-readable program code configured to authenticate is securely stored on the operably connected component.

58. (Previously Presented) The computer program product according to claim 54, further comprising computer-readable program code configured to authenticate the security core to the operably connected component.

59. (Canceled)

60. (Previously Presented) The computer program product according to claim 49, further comprising: computer-readable program code configured to detect whether the audio recording component and the at least one transformation component remain operably connected to the security core during operation of the recording and the computer-readable program code configured to transform; and computer-readable program code configured to mark the text stream as not authenticated if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core during operation of the recording and the computer-readable program code configured to transform.

61. (Previously Presented) The computer program product according to claim 55, further comprising: computer-readable program code configured to determine whether the audio recording component and the at least one transformation component have been authenticated to the security core; and computer-readable program code configured to abort the recording or the transforming if one or more of the audio recording component and the at least one transformation component has not been authenticated to the security core.

62. (Previously Presented) The computer program product according to claim 55, further comprising: computer-readable program code configured to determine whether the audio recording component and the at least one transformation component have been authenticated to the security core; and computer-readable program code configured to mark the text stream as not authenticated if one or more of the audio recording component and the at least one transformation component has not been authenticated to the security core.

63. (Previously Presented) The computer program product according to claim 49, wherein the computer-readable program code configured to securely provide further comprises computer-readable program code configured to digitally notorize, by the security core, the text stream.

64. (Previously Presented) The computer program product according to claim 49, wherein the computer-readable program code configured to securely provide further comprises computer-readable program code configured to provide an additional data stream that is associated with the text stream, wherein the additional data stream comprises a digital notarization, created by the security core, of the text stream.

65. (Previously Presented) The computer program product according to claim 63, wherein the computer-readable program code configured to digitally notarize further comprises: computer-readable program code configured to compute, by the security core, a hash value over the text stream; computer-readable program code configured to combine the hash value with a unique identifier of the audio recording component and of each of the at least one transformation components, thereby creating a combination data block; computer-readable program code configured to hash the combination data block; computer-readable program code configured to digitally sign the hashed combination data block with a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith; and computer-readable program code configured to provide the digitally signed hashed combination data block, along with the combination data block, as the digital notarization for the text stream, wherein the digital notarization cryptographically seals contents of the text stream and identifies the audio recording component and each of the at least one transformation components.

66. (Previously Presented) The computer program product according to claim 65, further comprising computer-readable program code configured to verify authenticity of the text stream by a receiver of the text stream and the digital notarization, using the public cryptographic key of the security core, and to conclude that the text stream is authentic if the verification succeeds.

67. (Previously Presented) The computer program product according to claim 66, wherein the computer-readable program code configured to verify authenticity further

comprises computer-readable program code configured to conclude that the text stream has not been tampered with if the verification succeeds.

68. (Previously Presented) The computer program product according to claim 66, wherein the computer-readable program code configured to verify authenticity further comprises computer-readable program code configured to determine the audio recording component and the at least one transformation component involved in creating the text stream by decoding the digitally signed hashed combination data block to reveal the unique identifiers thereof.

69. (Previously Presented) The computer program product according to claim 63, wherein: the computer-readable program code configured to transform the audio stream to a text stream further comprises: computer-readable program code configured to transform the audio stream to a digital stream by a first of the at least one transformation components which is an analog-to digital transformation component; and computer-readable program code configured to convert the digital stream to the text stream by a second of the at least one transformation components which is a speech recognition transformation component; and the computer-readable program code configured to digitally notarize the text stream further comprises: computer-readable program code configured to compute a hash over the text stream; computer-readable program code configured to combine the hash with unique identifiers of the audio recording component, the analog-to-digital transformation component, and the speech recognition transformation component; and computer-readable program code configured to digitally sign the combination using a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith.

70. (Previously Presented) The computer program product according to claim 63, wherein: the computer-readable program code configured to transform the audio stream to a text stream further comprises: computer-readable program code configured to transform the audio stream to a first digital stream by a first of the at least one transformation components

which is an analog-to-digital transformation component; computer-readable program code configured to convert the first digital stream to a first encoded text stream by a second of the at least one transformation components which is a speech recognition transformation component, wherein the speech recognition transformation component may be augmented by zero or more others of the at least one transformation components which are an authenticated speaker-specific speech recognition database and/or a lexical transformation component; and computer-readable program code configured to compress the first encoded text stream into the text stream using a third of the at least one transformation components which is a text compression transformation component; and the computer-readable program code configured to digitally notarize the text stream further comprises: computer-readable program code configured to compute a hash over the text stream, computer-readable program code configured to combine the hash with unique identifiers of: (1) the audio recording component; (2) the analog-to-digital transformation component; (3) the speech recognition transformation component; (4) the authenticated speaker-specific speech recognition database and/or the lexical transformation component, if they augmented the speech recognition transformation component; (5) the text compression transformation component; and computer-readable program code configured to sign the combination using a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith.

71. (Original) The computer program product according to claim 49, wherein the text stream is an ASCII text stream.

72. (Original) The computer program product according to claim 49, wherein the text stream is a Unicode text stream.